AUREXIS TRAINING AG · FREE RESOURCE

DORA Readiness Checklist

Governance and the five pillars of Regulation (EU) 2022/2554, applicable since 17 January 2025

Aligned with: Regulation (EU) 2022/2554 (DORA); RTS (EU) 2024/1774, 2024/1772, 2025/301; ITS (EU) 2024/2956

How to use: tick each item when it is in place and you can show evidence. Use the matching Aurexis Excel workbook to track owners, dates and evidence. Requirements are paraphrased by Aurexis; always work from the official text. Using this checklist does not guarantee certification or compliance.

Scope check

✓	Item
☐	We are a financial entity listed in Art. 2 (or an ICT third-party service provider to one) and know our competent authority.
☐	We have assessed whether the simplified ICT risk management framework (Art. 16) applies to us.
☐	We know whether we have been designated for threat-led penetration testing (Art. 26).
☐	We have identified our critical or important functions.

Governance

✓	Reference	Requirement
☐	Art. 5(2)	The management body defines, approves and oversees the ICT risk management framework and is accountable for it.
☐	Art. 5(2)	The management body approves the digital operational resilience strategy, ICT budget and the policy on ICT third-party arrangements.
☐	Art. 5(4)	Members of the management body keep their ICT risk knowledge current through regular training.
☐	Art. 6(4)	ICT risk is managed by a control function with sufficient independence (three lines of defence or internal risk model).
☐	Art. 6(8)	A digital operational resilience strategy is documented, including risk tolerance and ICT reference architecture.

ICT risk management

✓	Reference	Requirement
☐	Art. 6(1)	A documented ICT risk management framework exists (strategies, policies, procedures, protocols and tools).
☐	Art. 6(5)	The framework is reviewed at least yearly and after major ICT-related incidents or supervisory findings.
☐	Art. 6(6)	The framework is subject to regular internal audit by qualified auditors.
☐	Art. 7	ICT systems, protocols and tools are reliable, have sufficient capacity and are technologically resilient.
☐	Art. 8	Business functions, information assets and ICT assets are identified, classified and documented, including interconnections and dependencies.
☐	Art. 8	All sources of ICT risk are identified and assessed at least yearly, and on major change.
☐	Art. 8	Processes dependent on ICT third-party service providers are identified and mapped.

✓	Reference	Requirement
☐	Art. 9	Information security policies, access controls, strong authentication, patching and ICT change management are in place.
☐	Art. 10	Mechanisms detect anomalous activities and ICT network performance issues, with defined alert thresholds.
☐	Art. 11	An ICT business continuity policy and response and recovery plans exist and are tested.
☐	Art. 11	Crisis management and crisis communication arrangements are defined.
☐	Art. 12	Backup policies, restoration procedures and recovery methods are documented and tested; backups are segregated.
☐	Art. 13	Post-incident reviews feed lessons learned into the framework; staff receive ICT security awareness training.
☐	Art. 14	Communication plans cover clients, counterparts and the public for major incidents and vulnerabilities.
☐	Art. 16	Where eligible, the simplified ICT risk management framework is applied and documented.
☐	RTS (EU) 2024/1774	Detailed policies required by the RTS on the ICT risk management framework are in place.

Incident management

✓	Reference	Requirement
☐	Art. 17	An ICT-related incident management process detects, manages and notifies incidents, with early-warning indicators.
☐	Art. 17	All ICT-related incidents and significant cyber threats are recorded.
☐	Art. 17	Roles and responsibilities for incident scenarios are assigned; communication plans and escalation to senior management exist.
☐	Art. 18 / RTS (EU) 2024/1772	Incidents are classified using the regulatory criteria (clients affected, duration, geographic spread, data losses, criticality of services, economic impact).
☐	Art. 19 / RTS (EU) 2025/301	Major incidents are reported: initial notification within 4 hours of classification and no later than 24 hours after becoming aware; intermediate report within 72 hours of the initial notification; final report within one month of the latest intermediate report.
☐	Art. 19	Clients are informed without undue delay of major incidents affecting their financial interests.
☐	Art. 19(2)	A process exists for voluntary notification of significant cyber threats.

Resilience testing

✓	Reference	Requirement
☐	Art. 24	A risk-based digital operational resilience testing programme is established and maintained.
☐	Art. 24(6)	All ICT systems and applications supporting critical or important functions are tested at least yearly.
☐	Art. 25	Testing includes appropriate techniques (e.g. vulnerability assessments, network security, scenario-based, performance and penetration testing).
☐	Art. 24(5)	Issues found in testing are prioritised, classified and remediated.
☐	Art. 26	If designated by the competent authority, threat-led penetration testing (TLPT) is carried out at least every three years.
☐	Art. 27	Testers meet the independence and qualification requirements.

ICT third-party risk

✓	Reference	Requirement
☐	Art. 28(2)	A strategy on ICT third-party risk, including a policy on ICT services supporting critical or important functions, is adopted and reviewed.
☐	Art. 28(3) / ITS (EU) 2024/2956	A register of information on all ICT third-party contractual arrangements is maintained and provided to the competent authority on request.

✓	Reference	Requirement
☐	Art. 28(3)	The competent authority is informed in a timely manner of planned arrangements for critical or important functions.
☐	Art. 28(4)	Pre-contract assessment covers criticality, due diligence, conflicts of interest and supervisory conditions.
☐	Art. 28(7)	Contracts can be terminated in the circumstances listed by the regulation.
☐	Art. 28(8)	Exit strategies are documented and tested for ICT services supporting critical or important functions.
☐	Art. 29	ICT concentration risk is assessed before contracting.
☐	Art. 30	Contracts contain the mandatory provisions (service description, data locations, availability, incident assistance, cooperation with authorities, termination).
☐	Art. 30(3)	Contracts for critical or important functions add SLAs, notice periods, business continuity, TLPT participation, audit rights and exit provisions.

Information sharing

✓	Reference	Requirement
☐	Art. 45	Participation in cyber threat information-sharing arrangements is considered and, where joined, notified to the competent authority.

Major incident reporting clock

Report	Deadline (Art. 19, RTS (EU) 2025/301)
Initial notification	Within 4 hours of classification as major, and no later than 24 hours after becoming aware
Intermediate report	Within 72 hours of the initial notification (and when status changes significantly)
Final report	Within one month of the latest intermediate report

Weekend and holiday rules are set out in the RTS; check your competent authority's guidance.

Want to lead this yourself? The PECB DORA Lead Manager course teaches you to do it end to end, exam included. aurexistraining.com/training/dora-lead-compliance-manager